LOW VERSUS NO: SETTING A RISK APPETITE FOR INTERNAL FRAUD

While there is often zero tolerance expressed for internal fraud, the commensurate fraud risk framework required to adequately prevent and detect internal fraud can be challenging for organisations to achieve. Those organisations that have taken the leap and accepted a low appetite for internal fraud face another challenge: what the boundaries are and how a company should prepare for it. This session will discuss the different approaches between managing internal and external fraud as well as provide an understanding of an organisation’s fraud risk appetite.

TONY PRIOR, CFE, CAMS
Director, Ernst & Young
Australia

Tony Prior is a Director in Ernst & Young’s Fraud Investigation & Dispute Services team. He has experience in conducting both investigations and proactive financial crime services for the private and public sectors. He has spent the majority of his career working in financial services. Previously he was the head of financial crime at AMP Limited, Australia’s largest wealth manager, leading fraud risk, AML/CTF, sanctions, business security, and business continuity management teams. Now at EY he focuses exclusively within the financial-services sector providing proactive services to banks, insurers, superannuation companies, and boutique financial institutions.

Prior is well-credentialed, being a licensed investigator in all Australian states and New Zealand, a former Australian Federal Police agent, a CFE, a CAMS, and the Sydney Australia ACFE Chapter President. He has previously conducted a 12-month, in-country, anti-corruption engagement in Jakarta for the Indonesian government. He has also presented at several Asian and local conferences and authored several publications. In his 12 years in the Australian Federal Police he worked with several U.S. and U.K. law enforcement and posted overseas with the United Nations. He was awarded several commendations and service medals for his law enforcement activities.

The views expressed in this article are the views of the author, not Ernst & Young. This article provides general information, does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Liability limited by a scheme approved under Professional Standards Legislation.

©2015 Association of Certified Fraud Examiners
Introduction
Ask an executive in a typical financial institution about his organisation’s fraud risk appetite, and you will often get agreement that while there is conceptually some level of tolerance for external fraud, there is definitely no tolerance for internal fraud.

However, there is often a gap between that all too common expression of zero tolerance and the fraud risk framework that has been put in place. While the commonly held view is against accepting any level of internal fraud within the organisation, the commensurate controls and measures required to achieve that state are simply not there.

To adequately manage internal fraud, there should be a close alignment between the organisation’s prevention, detection and mitigation processes and its risk appetite. This refers to the extent to which an organisation is prepared to accept the possibility that risks will materialise. The lower there is an appetite for fraud risk and loss, the greater the number and coverage of processes that should be put in place. The quandary for financial institution executives boils down to a low fraud versus no fraud dichotomy--in other words, how much internal fraud is too much?

This paper will explore whether some level of internal fraud is inherently, and almost unconsciously, accepted by financial institutions, through the absence of adequate fraud risk frameworks. It will also examine the different dynamics in play between managing internal fraud versus external fraud.

The paper will draw upon examples and research from the financial services sector, reflecting my own experiences. It should be noted, though, that the concepts discussed apply
LOW VERSUS NO: SETTING A RISK APPETITE FOR INTERNAL FRAUD

across most industries, whether in the private or public (government) sectors.

Financial services are also well represented in the ACFE’s own research. In the most recent Report to the Nations on Occupation Fraud and Abuse,¹ the financial services sector featured prominently among the results:

- The banking and financial services sector had the highest reported cases of fraud, representing nearly 18 percent of all survey cases reported.
- Corruption was the highest fraud type for the banking and financial services sector.

Internal Fraud Versus External Fraud: Should They Be Managed Differently?

What is the difference between internal fraud risk management and external fraud risk management?

Let’s look first at how organisations manage external fraud. Consider a large financial institution with a heavy retail bank focus. A likely key performance indicator (KPI), both for the entire organisation and for individual executives in their performance agreements, is the level of customer satisfaction. To a certain extent, customer satisfaction is driven by retail customers’ individual experiences with the bank—how easy it is to transact; the level and nature of communication with the bank; adequacy and promptness of the bank’s response to queries or requests; and experiences the customer has with competitor institutions.

With this in mind, customer experience and fraud loss optimisation become a trade-off for the bank when managing external fraud losses. Take for example the choices a bank may face when deciding if a retail

¹ The Association of Certified Fraud Examiners, Report to the Nations on Occupation Fraud and Abuse (2014).
customer’s account card may have been compromised. In regard to the bank, how much loss is it prepared to incur so as not to disrupt the customer? With customer satisfaction and feedback being key performance indicators, the bank must decide whether to telephone or SMS the customer, decline the transaction, suspend or cancel the credit card, or allow the transaction to go through.

The financial institution’s risk appetite and associated controls and measures drive the nature of its response. Genuine transactions that are declined may impact customer experience, but if handled well, a telephone call or SMS about a legitimate transaction might actually create a positive experience, with the customer feeling that his bank is looking after him.

Financial institutions have become smart at increasing customer satisfaction and may “white-list” certain customers whose transactions will not face the same level of scrutiny or interruption. In these cases, the bank has made an informed choice to accept the associated level of risk.

If we turn our minds now to internal fraud, the same choices do not always present themselves. When combating internal fraud, customer experience is not the most significant consideration. The nature of internal fraud incidents does not often directly impact customers. This means there is a lesser chance of the customer detecting the fraud and contacting the bank—something that has not gone unnoticed by internal fraudsters!

It is often the impact on the brand that hurts a financial institution most when the institution suffers an internal fraud. Internal fraud and misconduct problems invariably attract media attention and, sometimes, even regulators or
government. Even relatively modest-sized frauds can be newsworthy. So while there may be some level of acceptance for financial loss, there will often be zero appetite for reputational impact or the risk of facing a regulatory or governmental inquiry.

The approach taken to setting an internal fraud risk appetite should therefore be designed not only to safeguard the financial institution and clients’ assets, but also to ensure minimal damage to the financial institution’s brand. The effect of this dual approach could be that control measures are designed to eradicate internal fraud but be more relaxed on potential external fraud where direct customer impact may come into play.

**Understanding an Organisation’s Risk Appetite Framework**

The *risk appetite* is the extent to which an organisation is prepared to accept the possibility that risks will materialise.

As part of the organisation’s overall approach to risk governance, the risk appetite framework must pass the *use test*: Do employees deep within the organisation’s structure appreciate and understand how the firm’s risk appetite both enables and constrains its day-to-day activities?

An effective embedded framework makes it clear what employees are accountable for in the context of the risk appetite of their business unit or activity.

**Setting the Fraud Risk Appetite**

There are a number of metrics that can be used, beyond dollar loss, when determining an acceptable level of fraud

---

LOW VERSUS NO: SETTING A RISK APPETITE FOR INTERNAL FRAUD

Risk. Forward loss—what the organisation is willing to sustain from any source in a severe environment—is a common measure that allows business units to be compared to one another to set an agreed risk appetite. Other metrics include:

- Incidents—the number of internal fraud or code of conduct incidents
- Attempts—the number of near misses or fraud attempts that failed
- Customer complaints—complaints concerning an actual fraud occurrence, complaints about the transaction or accounts being frozen, or complaints about delays in recompensing a fraud loss
- Employee training—the percentage of employees that have completed mandatory fraud training
- Genuine declines—the number of genuine transactions that were falsely classified as fraud and declined

Importantly, cultural risk appetite plays a significant role in managing internal fraud and misconduct. Recent high profile conduct failings and the associated regulatory scrutiny have placed more emphasis on risk culture. Organisations are expected to review and assess their risk culture and then make changes to improve it.

In this environment, consideration should also be given to activities designed to impact behaviour. The culture of the financial institution may drive certain behaviours which impact the perception of the level of internal fraud acceptability. Understanding this is as critical as analysing the absolute metrics.

Qualitative measures designed to reinforce the organisational tone therefore become just as important.

---

Continuous reinforcement through communications and training, alongside assessing, tracking, and monitoring individual progress against risk framework plans strengthen risk culture.

To help achieve this, a financial institution may, for example, mandate that all allegations of internal fraud will be subject to its disciplinary procedures regardless of how trivial or dated the allegation appears. Aligning employees’ behaviour with the financial institution’s risk objectives can also be achieved through linking reward with the objectives the institution wishes to accept.

**Fraud Controls and Activities**

Once the acceptable level of risk appetite has been determined, resources can then be directed to particular fraud processes and risk management activities as needed. Fraud risk resource allocation can be broadly categorised into two activities:

1. *Fraud investigation (reactive measures).*
   Financial institutions often base their stated zero tolerance for internal fraud on the grounds that they investigate all fraud matters. This argument is flawed, because it ignores the application of the proactive measures necessary to reflect a true low, or zero, appetite for fraud. While appropriate reactive responses are certainly required, they don’t take into account the activities required to deter, prevent, or detect fraud earlier on.

2. *Fraud risk management (proactive measures).*
   The correlation between proactive measures and expressed risk appetite is generally less evident in financial institutions than the reactive measures. Too often, we see a stated zero tolerance for internal fraud, yet the proactive measures are either ineffective, do not cover the entire organization, or are completely lacking.
For example, an employee might be able to fraudulently alter a payment file to redirect inward contributions to an incorrect account. Timely reconciliation of money (contributions) to data (contribution file) and activated audit logs should be operating to help detect this and, depending on the risk rating, proactive forensic data analytics might also be warranted.

**Putting Fraud Risk Appetite into Operation**

Where should financial institutions start when it comes to determining an appropriate level of internal fraud risk and putting a mitigating framework in place that aligns to that level?

Some financial institutions start at a low base in terms of their risk management maturity or level of sophistication. Their fraud risk appetite may be nothing more than planning for next year’s fraud losses to not exceed this year’s.

Risk appetite for fraud loss should be a standard part of a financial institution’s risk management planning cycle. Calculations should be based on robust management information of actual experiences and predicted risks. It should also consider the risks and rewards of any planned new products and channels. Once the level of fraud risk appetite has been agreed on, it should then be communicated across the institution and the appropriate oversight procedures should be put in place.

At the other end of the cycle, reporting should occur in line with the pre-defined risk appetite with the appropriate intervention when both positive and negative variances to the plan occur. Socialisation of notable results should be supported with strong messages and reinforced at the top of the institution.
A recent survey\(^4\) noted several key factors critical to successfully translating risk appetite into operation. These include:

- **Applying a top-down and bottom-up approach.** While the Board approves the risk appetite, senior executives and managers must be involved in its development. The appetite should be measurable and executable—a simple and practical framework that business units can understand.

- **Linking appetite to business strategy and planning.** An organisation’s budgets and revenue projections cannot be determined unless the activities and transactions needed to get there are compliant with the risk appetite statement. Controls and other measures should be developed at a business unit level to meet the overall risk appetite of the organisation.

- **Establishing a clear reporting and accountability process.** Tracking individual executive and leader performance to evaluate how they have performed is important. Clearly defined escalation processes for breaches provide real consequences to those responsible for decision making.

### Finding the Sweet Spot Between Low Appetite and No Appetite for Internal Fraud

When there is a zero tolerance policy for internal fraud, the commensurate fraud risk framework required to adequately prevent and detect internal fraud can be challenging for financial institutions to achieve.

On the other hand, those financial institutions that have taken the leap and accepted a low appetite for internal fraud face another challenge: How do they manage the optics of a

---

low appetite and still communicate the message to employees that it is not “open slather”?

A key plank in a fraud risk framework is strong deterrence, with overt condemnation of internal fraud and "tone at the top” messages and behaviours. Openly expressing trust in your employees can be a powerful message.

It all comes down to the way risk appetite is operationalised and embedded in the organisation’s day to day business. Organisations need to communicate the acceptance that a certain level of internal fraud will probably occur as a commercial reality of doing business without sending the wrong message.

**Keeping Pace With Change**

Regulators and other external stakeholders are becoming increasingly interested in organisations’ risk appetite statements. External scrutiny is evident when internal fraud and associated misconduct incidents occur, with difficult questions asked about how and why it happened. Why was there no adequate oversight? Why didn’t the controls detect it earlier?

Keeping pace with change requires a two pronged approach:

1. **Monitoring.** Use an appetite statement that is both quantitative and qualitative in nature with agreed upon metrics. Include triggers for management action and the appropriate escalation.

2. **Review and refresh.** Fraud risk management is not a set-and-forget exercise. Like other operational risks, fraud risk is fluid, and ongoing monitoring is required to capture material changes to existing fraud risk profiles. Many financial institutions already de-risk their books and end customer relationships when they present too
high a risk. Upfront declines of new client applications are now also becoming part of the broader fraud risk framework.

Conclusion
There is no quick fix, one-size-fits-all approach when it comes to finding the sweet spot between low appetite and no appetite for internal fraud. It will vary for each individual financial institution.

But there are some common denominators. Those financial institutions with the greatest success in managing internal fraud risk are able to clearly articulate their fraud risk appetite and then operationalise and embed it into the business. They also engage a mature fraud risk management framework that utilises proactive measures to deter, prevent and detect fraud, rather than solely relying upon reactive measures.

Organisations that are able to get this balance right will be well-positioned to manage their internal fraud risk and adapt to changing circumstances.
<table>
<thead>
<tr>
<th>LOW VERSUS NO: SETTING A RISK APPETITE FOR INTERNAL FRAUD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>